UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/741,798	12/19/2003	Susan Pittman Dark	58895/P001C1/10316486	5599

29053 7590 08/27/2009

FULBRIGHT & JAWORSKI L.L.P
2200 ROSS AVENUE
SUITE 2800
DALLAS, TX 75201-2784

EXAMINER	
RUTKOWSKI, JEFFREY M	
ART UNIT	**PAPER NUMBER**
2416	

MAIL DATE	DELIVERY MODE
08/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/741,798	DARK, SUSAN PITTMAN	
	Examiner	Art Unit	
	JEFFREY M. RUTKOWSKI	2416	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 June 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30,33-50 and 54-74* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30,33-50 and 54-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 31-32 and 51-53 have been cancelled.

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 06/29/2009 has been entered.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the first and second paragraphs of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. **Claim 8** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It is not clear what is meant by dynamically changing gathered information based on currently gathered information.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

5. **Claims 1-3, 8-9, 11, 15-18, 22, 26-28, 32-35, 40-41, 44-45, 47-48, 52-55, 59, 63-67 and 74** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauff et al. (US Pat 6,415,321), hereinafter referred to as Gleichauff in view of Eschelbeck et al. (US Pat 6,611,869), hereinafter referred to as Eschelbeck and Smith et al. ("Operating Firewalls Outside the LAN Perimeter").

6. For **claims 1, 33 and 65**, Gleichauff discloses a network environment where packets that are received over the Internet (temporally available network) is received at a router **14** (gateway router) that serves the purpose of directing packets via firewall **16** to either a web server **30** or a file server **34** (receiving devices) based upon address information **[col. 4 line 67 to col. 5 line 15]**. Gleichauff's network environment further includes an Intrusion Detection System (IDS) **18** and a domain mapping system **46 [figure 3]**. The domain mapping system **46**, which is part of a monitoring system, has an acquisition engine **48** that is used to gather operational information which, inter alia, includes such as Operating System (OS) type, services offered and potential vulnerabilities, on network devices (receiving devices). The information is gathered by the acquisition engine **48** via actively querying the network devices, polling or having the network devices push information **[col. 5 line 45 to col. 6 line 30]**.

7. Gleichauff discloses the IDS **18** uses the information stored in the domain mapping system **46** to provide protection for the network devices, such as file server **34 [col. 6 lines 48-65]**. Gleichauff does not disclose what happens if the IDS **18** detects an attack. Eschelbeck discloses when an attack is detected by an IDS, a message is sent to the firewall via network (feedback network) to have the firewall update it's Access Control List (ACL) (modify operational characteristics) to prevent traffic from the source of the attack from entering the network **[col. 6 lines 4-25]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauff's invention to provide an active security management environment **[Eschelbeck, abstract]**.

8. The combination of Gleichauff and Eschelbeck disclose the active security management of a firewall. The combination of Gleichauff and Eschelbeck do not disclose the active security management of a gateway router. Smith discloses traditionally routers performed firewall functions via ACL **[Section 1 2nd paragraph]**. Smith also discloses the use of gateway-firewalls to protect networks **[Section 3, Section 3.4 last paragraph]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router in Gleichauff's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

9. Specifically for **claim 65**, Gleichauff discloses the IDS **48** can be placed in any location in the network, including a firewall **[col. 5 lines 10-13]**. Which suggests an architecture where packets are stored (database for future delivery) and then scanned before being transferred to the destination device.

10. For **claims 2, 34 and 66**, Gleichauff discloses that Simple Network Management Protocol (SNMP) queries (certain data contained in one or more messages) can be used to gather information **[col. 6 lines 23-25]**.

11. For **claims 3, 18, 35, 55 and 67**, Gleichauf discloses the use of signature matching, where packets are compared to "attack signatures" (pre-established criteria), and pattern matching are known methods to detect attacks **[col. 1 lines 25-30]**.

12. Gleichauf does not disclose setting limits. Smith suggests the setting of limits applying to a volume of data by disclosing an firewall and IDS system that detects Denial-of-Service attacks **[Section 1 page 494]**. Since DoS attacks work by causing a victim device to overflow its buffers by sending a large number of requests in a short amount of time, it would have been obvious to a person of ordinary skill in the art at the time of the invention to set limits based on attack signatures (pre-established criteria) to stop a DoS attack before the victim device "crashes".

13. Glecichau also does not disclose adjusting ACL rules when an DoS attack is detected. Smith discloses a system that detects DoS attacks and routers traditionally performed firewall functions via ACL **[Section 1 page 494, Section 1 2nd paragraph]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active security management on the ACL of a gateway router based upon set limits in Gleichauff's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

14. For **claim 8**, Gleichauf's invention takes into account that information changes dynamically by actively collecting information from network devices **[col. 5 line 45 to col. 6 line 30]**.

15. For **claims 9 and 41**, Gleichauff does not disclose the blocking of certain packets from reaching a destination. Eschelbeck discloses ACL is updated to prevent any more traffic from the source of the attack from entering the network **[col. 6 lines 4-25]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauff's invention to provide an active security management environment **[Eschelbeck, abstract]**.

16. For **claims 11 and 74**, Gleichauf suggests an IDS **18**, which is part of a monitoring system, that can be used to monitor traffic leaving a network device (receiving device) because the IDS **18** monitors network traffic as a whole **[col. 5 lines 5-8, figure 3]**.

17. Gleichauf does not disclose a gateway router where the ACL is modified according to outbound traffic. Smith contemplates the use of outbound traffic gateway firewalls **[Section 4]**. Given that Smith is concerned with stopping attacks as close to the source as possible and ACLs are used to keep one node from accessing another node **[Sections 1 and 3.4]**, it would have been obvious to a person of ordinary skill in the art at the time of the invention to block egress traffic via router gateway ACL to prevent an attack from the inside of the network.

18. For **claims 15, 27, 45 and 64**, Gleichauff does not disclose changing ACL rules in a remote system. Smith discloses that in a corporate network, when a firewall detects an attack, messages are sent to remote gateway-firewalls (remote communication system) to have the attacker blocked (modify operational characteristics) **[Section 3.4]**. It would have been obvious

to a person of ordinary skill in the art at the time of the invention to perform remote ACL management of a gateway router in Gleichauff's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

19. For **claims 16 and 52-53**, Gleichauff discloses the use of an enterprise system **[figure 3]**.

20. For **claims 17, 28, 48 and 54**, Gleichauff discloses an IDS **18** (system for tracking data flow; means for real time review) that is used to perform a pattern matching (identification of a specific data pattern; means for comparing) **[col. 1 lines 25-30, figure 3]**.

21. Gleichauff discloses the IDS **18** uses the information stored in the domain mapping system **46** to provide protection for the network devices, such as file server **34 [col. 6 lines 48-65]**. Gleichauff does not disclose what happens if the IDS **18** detects an attack. Eschelbeck discloses when an attack is detected by an IDS, a message is sent to the firewall via network (send instructions from time to time; means for feeding) to have the firewall update it's ACL to prevent traffic from the source of the attack from entering the network **[col. 6 lines 4-25]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Eschelbeck's IDS in Gleichauff's invention to provide an active security management environment **[Eschelbeck, abstract]**.

22. The combination of Gleichauff and Eschelbeck disclose the active security management of a firewall. The combination of Gleichauff and Eschelbeck do not disclose the active security management of a gateway router (control device). Smith discloses traditionally routers performed firewall functions via ACL **[Section 1 2nd paragraph]**. Smith also discloses the use of gateway-firewalls to protect networks **[Section 3, Section 3.4 last paragraph]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to perform active

security management on the ACL of a gateway router in Gleichauff's invention to block attacks as close to the source of the attack as possible **[Section 3, 2nd paragraph]**.

23. For **claims 22 and 59**, Gleichauff discloses the use of an hypercube storage **50** (database).

24. For **claims 26, 32 and 63**, figure 3 of Gleichauff shows the gateway router **14** of the local site (gateway unique to a particular location) is the gateway router whose ACL is modified

25. For **claim 40**, Gleichauf discloses a pattern analysis technique where packets are compared to "attack signatures" **[col. 1 lines 25-30]**.

26. For **claim 44**, figure 3 of Gleichauff shows the gateway router **14** of the local site (particular location) is the gateway router whose ACL is modified.

27. For **claim 47**, Gleichauff discloses gathered network information is stored in a hypercube storage **50 [figure 3]**.

28. **Claims 5, 21, 37, 58 and 69** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauff in view of Eschelbeck and Smith as applied to **claims 3, 18, 28, 35 and 67 respectively** above, and further in view of Kouznetsov (US Pat 6,725,377).

29. For **claims 5, 21, 37, 58 and 69**, the combination of Gleichauff, Eschelbeck and Smith does not disclose the manual adjustment of thresholds. Kouznetsov discloses a user decides which attack signatures are to be included in the profile, which results in a manual adjustment of detection thresholds **[col. 2 lines 53-65]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use manually adjusted limits in Gleichauff's invention to take into account new attack patterns **[Kouznetsov, abstract]**.

30. **Claims 6-7, 10, 12-14, 20, 23-25, 38-39, 43, 46, 57, 60-62, 70-73** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauff in view of Eschelbeck and Smith as applied to **claims 1, 17, 18, 29, 33 and 65 respectively** above, and further in view of Conklin et al. (US Pat 5,991,881) hereinafter referred to as Conklin.

31. For **claims 6, 38 and 70**, the combination of Gleichauff, Eschelbeck and Smith discloses the gathering of information from a network device. The combination of Gleichauff, Eschelbeck and Smith does not disclose the statistical comparison of gathered information. Conklin discloses a attack detection process where captured packets (gathered information) is compared against historical information that was collected over time **[col. 7 lines 50-55]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauff's invention to use of artificial intelligence to detect attacks **[Conklin, col. 7 line 53]**.

32. For **claims 7, 20, 39, 57 and 71**, the combination of Gleichauff, Eschelbeck and Smith does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior **[col. 7 lines 50-55]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauff's invention to "feed" the artifical intelligence engine.

33. For **claims 10, 43 and 73**, the combination of Gleichauff, Eschelbeck and Smith does not disclose the storage of received packets. Conklin discloses an IDS process where incoming packets is stored **[figure 7]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to use Conklin's detection mechanism in Gleichauff's invention to use

of artificial intelligence to detect attacks **[Conklin, col. 7 line 53]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to store packet information in Gleichauff's invention to allow for the use of artificial intelligence to detect attacks **[Conklin, col. 7 line 53]**.

34. For **claims 12, 23, 46 and 60**, the combination of Gleichauff, Eschelbeck and Smith does not disclose gathering packet information. Conklin discloses packets are collected and statistical information from the packets is stored (information about the history of the packets) **[figure 7]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to gather packet information in Gleichauff's invention to use artificial intelligence to detect an attack.

35. For **claims 13, 24 and 61**, Gleichauff discloses the storing information to be used by an IDS **18** system **[col. 6 lines 50-55, figure 3]**.

36. For **claims 14, 25 and 62**, Gleichauff discloses the IDS **18** obtains a vulnerabilities list (selected data) that is grouped by OS (parameters of receiving device) and incidence **[col. 6 lines 62-65]**.

37. For **claim 72**, Gleichauff discloses a pattern analysis technique where packets are compared to "attack signatures" **[col. 1 lines 25-30]**.

38. **Claims 30 and 50** are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauff in view of Eschelbeck, Smith and Kouznetsov as applied to **claims 29 and 49 respectively** above, and further in view of Conklin.

39. For **claims 30 and 50**, the combination of Gleichauff, Eschelbeck, Smith and Kouznetsov does not disclose the gathering of statistics to reflect normal behavior. Conklin disclosure that

artificial intelligence techniques can be used to detect attacks, suggests gathering statistics to reflect normal behavior **[col. 7 lines 50-55]**. It would have been obvious to a person of ordinary skill in the art at the time of the invention to collect statistics to reflect normal behavior in Gleichauff's invention to "feed" the artificial intelligence engine.

Response to Arguments

40. Response to arguments in Section D of the response filed on 06/29/2009.

41. The indefiniteness rejection was maintained for **claim 8** because **claim 8** is still pending and was not cancelled as indicated on page 17 of the Applicant's response.

42. Response to arguments for Section F of the response filed on 06/29/2009.

43. The argument with respect to Gleichauff's firewall restricting traffic that is already in the internal network is not persuasive because Gleichauff's firewall also restricts traffic in the inbound direction (see col. 5 lines 1-5).

44. The arguments with respect to the proposed combination of Gleichauff and Smith not being proper because Smith changes Gleichauff's architecture are not persuasive. Smith does not change the physical arrangement of Gleichauff's invention. What Smith teaches is to block inbound traffic at the gateways nearer to the source of the attack to keep the attack as far away from the destination attack as possible (page 496 Section 3 2nd paragraph). Smith's invention still needs a firewall and a gateway. For example, if a firewall detects an attack a message is sent to the gateway to block the attack (page 498 last paragraph before Section 4). In Gleichauff's invention, the gateway that is as close to the source as possible is the router **14** (see figure 3). The proposed modification to Gleichauff was to use an ACL in router **14** to block the incoming traffic as taught by Smith.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY M. RUTKOWSKI whose telephone number is (571)270-1215. The examiner can normally be reached on Monday - Friday 7:30-5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kwang Yao can be reached on (571) 272-3182. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeffrey M Rutkowski/
Examiner, Art Unit 2416

/Steven HD Nguyen/
Primary Examiner, Art Unit 2416